Amendments to the Claims

Claim 1 (currently amended): A computer program product embodied on computer readable media readable by a computing system in a computing environment, for enforcing security policy using style sheet processing, comprising:

computer-readable program code means for obtaining an input document;

~~one or more stored policy enforcement objects, wherein each of said stored policy enforcement objects specifies a security policy to be associated with zero or more elements of said input document;~~

computer-readable program code means for obtaining a Document Type Definition (DTD) ~~corresponding to~~ that defines elements of said input document, wherein: (1) an attribute of at least one element defined in said DTD ~~has been augmented with one or more~~ references ~~to selected ones~~ one of a plurality of ~~said~~ stored policy enforcement objects; (2) more than one of said references may reference a single stored policy enforcement object; and (3) each of said stored policy enforcement objects specifies a visibility policy for said referencing element or elements, said visibility policy identifying an encryption requirement for all elements having that visibility policy and a community whose members are authorized to view those elements;

computer-readable program code means for applying one or more style sheets to said input document, thereby adding markup notation to each element of said input document for which said element definition in said DTD references one of said stored policy enforcement objects specifying a visibility policy with a non-null encryption requirement, resulting in creation of an interim transient document that indicates elements of said input document which are to be encrypted; and

computer-readable program code means for creating an output document in which each element of said interim transient document for which markup notation has been added is encrypted in a manner that enables a clerk process associated with a group that is a community member authorized to view that element to use key distribution material associated with the output document when decrypting the encrypted element.

~~an augmented style sheet processor, wherein said augmented processor further comprises:~~

~~computer-readable program code means for loading said DTD;~~

~~computer-readable program code means for resolving each of said one or more references in said loaded DTD;~~

~~computer-readable program code means for instantiating said policy enforcement objects associated with said resolved references;~~

~~computer-readable program code means for executing selected ones of said instantiated policy enforcement objects during application of one or more style sheets to said input document, wherein a result of said computer-readable program code means for executing is an interim transient document reflecting said execution;~~

~~computer-readable program code means for generating one or more random encryption keys;~~

~~computer-readable program code means for encrypting selected elements of said interim transient document, wherein a particular one of said generated random encryption keys may be used to encrypt one or more of said selected elements, while leaving zero or more other elements of said interim transient document unencrypted;~~

~~computer-readable program code means for encrypting each of said one or more random encryption keys; and~~

~~computer-readable program code means for creating an encrypted output document comprising said zero or more other unencrypted elements, said selected encrypted elements, and said encrypted encryption keys;~~

~~computer-readable program code means for requesting, from a user or process on a client device, said encrypted output document, wherein said user or process is a member of a particular group authorized to view at least one of said selected encrypted elements;~~

~~computer-readable program code means for receiving said requested output document at said client device; and~~

~~an augmented document processor executed on said client device, comprising:~~

~~computer-readable program code means for contacting a clerk of said particular group for decryption of selected ones of said encrypted encryption keys; and~~

~~computer-readable program code means for decrypting said requested output document using said decrypted selected ones of said encrypted encryption keys, thereby creating a result document.~~

Claim 2 (currently amended): The computer program product according to Claim 1, further comprising computer-readable program code means for rendering said output ~~result~~ document on ~~said client~~ a client device.

Claim 3 (currently amended): The computer program product according to Claim 1, wherein said markup notation in said interim transient document comprises ~~one or more encryption~~ tags ~~identifying elements needing encryption~~ of a markup language.

Claim 4 (original): The computer program product according to Claim 1, wherein said input document is specified in an Extensible Markup Language (XML) notation.

Claim 5 (currently amended): The computer program product according to Claim 4, wherein said output ~~result~~ document is specified in said XML notation.

a19

Claim 6 (currently amended): The computer program product according to Claim 1, wherein said stored policy enforcement objects further comprise computer-readable program code means for overriding a method for evaluating said elements of said input document, and wherein said computer-readable program code means for applying said one or more style sheets ~~executing~~ further comprises computer-readable program code means for invoking ~~executing~~ said computer-readable program code means for overriding, thereby causing said markup notation to be added.

Claim 7 (original): The computer program product according to Claim 6, wherein said style sheets are specified in an Extensible Stylesheet Language (XSL) notation.

Claim 8 (original): The computer program product according to Claim 7, wherein said method is a value-of method of said XSL notation, and wherein said computer-readable program code means for overriding said value-of method is by subclassing said value-of method.

Claim 9 (currently amended): The computer program product according to Claim ~~6 or Claim 8~~, wherein:

said ~~overridden~~ overriding method comprises:

computer-readable program code means for generating said markup notation as encryption tags; and

a19

computer-readable program code means for inserting said generated encryption tags into said interim transient document to surround elements of said interim transient document for which said visibility policy of said elements in said input document have said non-null ~~are determined to require~~ encryption requirement; and

said computer-readable program code means for creating said output document further comprises computer-readable program code means for encrypting ~~selected elements encrypts~~ those elements surrounded by said inserted encryption tags.

Claim 10 (canceled)

Claim 11 (currently amended): The computer program product according to ~~Claim 10, wherein~~ Claim 1, wherein said encryption requirement further comprises specification of an encryption algorithm to be used when encrypting elements having that visibility policy.

Claim 12 (currently amended): The computer program product according to ~~Claim 10, wherein~~ Claim 1, wherein said encryption requirement further comprises specification of an encryption algorithm strength value to be used when encrypting elements having that visibility policy.

Claim 13 (currently amended): The computer program product according to ~~Claim 10, wherein~~ Claim 1, wherein said computer-readable program code means for creating said output document further comprises:

computer-readable program code means for generating a distinct symmetric key for each unique one of said communities identified by said visibility policy in said stored policy objects for each of said elements of said input document; and

~~said~~ computer-readable program code means for encrypting each of said distinct symmetric keys to create member-specific versions thereof, further comprising:

computer-readable program code means for determining whether each of said members of said community for which said distinct symmetric key was generated is an individual or a group; and

computer-readable program code means for encrypting a separate version of said distinct symmetric key for each determined individual and for a clerk process associated with each determined group. ~~encryption keys further comprises computer-readable program code means for encrypting a different version of each of said random encryption keys for each of said one or more members of each of zero or more of said communities which uses said encryption key , and~~

~~wherein each of said different versions is encrypted using a public key of said community member for which said different version was encrypted.~~

Claim 14 (currently amended): The computer program product according to ~~Claim 10, wherein said encryption requirement may have a null value to indicate that said specified security policy does not require encryption.~~ Claim 13, wherein said computer-readable program code means for encrypting a separate version of said distinct symmetric key creates one of said member-specific versions using, as input, a public key of one of said determined individuals or a public key of said clerk process.

a19

Claim 15 (currently amended): The computer program product according to Claim 1, wherein said ~~computer-readable program code means for encrypting selected~~ encrypted elements in said created output document are encrypted using ~~uses~~ a cipher block chaining mode encryption process.

Claim 16 (currently amended): The computer program product according to Claim 13, further comprising:

computer-readable program code means for creating a key class for each of said unique ~~community~~ communities, wherein said key class is associated with each of said encrypted elements of said output document for which members of this unique community ~~is an~~ are authorized ~~viewer~~ viewers, and wherein said key class comprises: (1) ~~a strongest~~ an encryption algorithm identifier and key length used when encrypting ~~requirement of~~ said associated encrypted

elements; (2) an identifier of each of said members of said unique community; and (3) one of said ~~different~~ member-specific versions of said encrypted symmetric ~~encryption~~ key for each of said identified community members~~; and~~

~~wherein:~~

~~said computer-readable program code means for generating said one or more random encryption keys generates a particular one of said random encryption keys for each of said key classes, and wherein each of said different versions in a particular key class is encrypted from said generated encryption key generated for said key class; and~~

~~said computer-readable program code means for encrypting selected elements uses that one of said partieular random encryption keys which was generated for said key class with which said selected element is associated~~.

Claim 17 (currently amended): The computer program product according to Claim 13, further comprising ~~wherein~~:

~~said~~ computer-readable program code means for decrypting, for an individual user or process that is a member of one or more of said determined groups, only those encrypted elements in said ~~requested~~ output document for which any of said one or more of said determined groups is one of said authorized community members, further ~~comprises~~ comprising:

computer-readable program code means for expanding said ~~one or more~~ determined groups ~~of said communities~~ to determine said individual users or processes that are group members in each of said expanded groups;

computer-readable program code means for identifying ~~determining~~ one or more of said expanded groups ~~communities~~ of which said individual ~~requesting~~ user or process is one of said ~~expanded~~ group members;

computer-readable program code means for decrypting, by said clerk process for each of said ~~determined communities~~ identified groups, said ~~different~~ member-specific version of said ~~random encryption~~ symmetric key ~~which was encrypted using said public key of said one member, wherein said one member is said expanded group of which said requesting user or process is one of said expanded group members~~, thereby creating a decrypted key for each of said ~~determined communities~~ identified groups; and

a19 computer-readable program code means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document using said decrypted keys, wherein said selected ones of said encrypted elements are those which were encrypted for one of said ~~determined communities~~ identified groups; ~~and~~

~~said computer-readable program code means for rendering further comprises:~~

~~computer-readable program code means for rendering said decrypted selected ones and said other unencrypted elements~~.

Claim 18 (currently amended): The computer program product according to Claim 17, wherein:

said computer-readable program code means for encrypting a separate version uses a public key of said clerk process as input when creating said member-specific version for said clerk process;

said computer-readable program code means for decrypting said member-specific version of said symmetric key further comprises:

~~said~~ computer-readable program code means for contacting said ~~group~~ clerk process, further ~~comprises~~ comprising:

computer-readable program code means for programmatically locating said ~~group~~ clerk process; and

computer-readable program code means for establishing a session between ~~said client~~ a client device used by said individual user or process and said ~~group~~ clerk process;

~~said computer-readable program code means for decrypting said different version for each of said determined communities further comprises:~~

a19

computer-readable program code means for digitally signing said ~~different~~ member-specific version by said individual ~~requesting~~ user or process, thereby creating a first digital signature;

computer-readable program code means for sending said first digital signature and said ~~different~~ member-specific version to said ~~group~~ clerk process on said session;

computer-readable program code means for receiving said sent first digital signature and said ~~different~~ member-specific version by said ~~group~~ clerk process;

computer-readable program code means for verifying said first digital signature by said ~~group~~ clerk process;

computer-readable program code means for verifying, by said ~~group~~ clerk process, that said ~~requesting~~ individual user or process is one of said ~~authorized~~ members of said ~~determined community~~ identified group associated with said ~~different~~ member-specific version;

computer-readable program code means for decrypting said ~~different~~ member-specific version using a private key of said ~~one member which~~ clerk process, wherein said private key is associated with said public key ~~which was used for encryption~~ of said clerk process;

computer-readable program code means for re-encrypting said decrypted ~~different~~ member-specific version using a public key of said individual ~~requesting~~ user or process, thereby creating a re-encrypted key;

computer-readable program code means for digitally signing said re-encrypted key by said ~~group~~ clerk process, thereby creating a second digital signature;

computer-readable program code means for returning said second digital signature and said re-encrypted key from said ~~group~~ clerk process to said client device on said session;

computer-readable program code means for receiving said second digital signature and said re-encrypted key at said client device;

computer-readable program code means for verifying said second digital signature at said client device; and

computer-readable program code means, operable on said client device, for decrypting said received re-encrypted key using a private key of said individual ~~requesting~~ user or process, creating said decrypted key; and

said computer-readable program code means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document is executed at said client device using said decrypted key.

Claim 19 (currently amended): The computer program product according to Claim 13, ~~wherein~~ further comprising:

~~said~~ computer-readable program code means for decrypting, for an individual user or process that is a member of one of said determined groups, only those encrypted elements in said ~~requested~~ output document for which any of said one or more of said determined groups is one of said authorized community members, further ~~comprises~~ comprising:

computer-readable program code means for expanding said ~~one or more~~ determined groups ~~of said communities~~ to determine said individual users or processes that are group members in each of said expanded groups;

a19

computer-readable program code means for identifying ~~determining~~ one or more of said expanded groups ~~communities~~ of which said individual ~~requesting~~ user or process is one of said ~~expanded~~ group members; and

computer-readable program code means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document, wherein said selected ones of said encrypted elements are those which were encrypted for one of said identified groups ~~determined communities; and~~

~~said computer readable program code means for rendering further comprises:~~

~~computer readable program code means for rendering said returned decrypted elements and said other unencrypted elements~~.

Claim 20 (currently amended): The computer program product according to Claim 19, further comprising ~~wherein~~:

~~said~~ computer-readable program code means for contacting said ~~group~~ clerk process, further ~~comprises~~ comprising:

computer-readable program code means for programmatically locating said ~~group~~ clerk process; and

computer-readable program code means for establishing a mutually-authenticated secure session between ~~said client~~ a client device used by said individual user or process and said ~~group~~ clerk process; and wherein:

said computer-readable program code means for encrypting a separate version uses a public key of said clerk process as input when creating said member-specific version for said clerk process; and

said computer-readable program code means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document further comprises:

computer-readable program code means for locating said member-specific ~~different~~ version of said ~~random encryption~~ symmetric key which was encrypted using said public key of said ~~one member~~ clerk process, wherein said clerk process ~~one member~~ is associated with a ~~said expanded~~ group of which said individual ~~requesting~~ user or process is a group member; ~~one of said expanded group members;~~

computer-readable program code means for sending said located member-specific ~~different~~ version to said ~~group~~ clerk process, along with an element encrypted with said member-specific ~~different~~ version, on said secure session;

computer-readable program code means for receiving said sent member-specific ~~different~~ version and said element by said ~~group~~ clerk process;

computer-readable program code means for verifying, by said ~~group~~ clerk process, that said ~~requesting~~ individual user or process is one of said ~~authorized~~ members of said ~~determined community~~ identified group associated with said member-specific ~~different~~ version;

computer-readable program code means for decrypting said member-specific ~~different~~ version using a private key of said clerk process; ~~one member which is associated with said public key which was used for encryption;~~

computer-readable program code means for decrypting said element using said decrypted member-specific ~~different~~ version; and

computer-readable program code means for returning said decrypted element from said ~~group~~ clerk process to said client device on said secure session.

Claim 21 (currently amended): The computer program product according to Claim 16, wherein: said computer-readable program code means for encrypting a separate version uses a public key of said clerk process as input when creating said member-specific version for said clerk process; and further comprising:

~~said~~ computer-readable program code means for contacting said ~~group~~ clerk process, further ~~comprises~~ comprising:

computer-readable program code means for programmatically locating said ~~group~~ clerk process; and

computer-readable program code means for establishing a mutually-authenticated secure session between ~~said client~~ a client device used by said individual user or process and said ~~group~~ clerk process;

~~said~~ computer-readable program code means for decrypting, for an individual user or process that is a member of one of said determined groups, only those encrypted elements in said ~~requested~~ output document for which any of said one or more of said determined groups is one of said authorized community members, further comprising: ~~further comprises:~~

computer-readable program code means for expanding said ~~one or more~~ determined groups ~~of said communities~~ to determine said individual users or processes that are group members in each of said expanded groups;

computer-readable program code means for identifying ~~determining~~ one or more of said key classes which identify said ~~requesting~~ individual user or process as one of said ~~expanded~~ group members;

computer-readable program code means for decrypting, for each of said determined key classes, said member-specific ~~different~~ version of said symmetric ~~random encryption~~ key in said key class which was encrypted using said public key of said clerk process ~~one member~~, wherein said computer-readable program code means for decrypting uses a private key of said clerk process ~~one member which is associated with said public key which was used for encryption~~, thereby creating a decrypted key; and

computer-readable program code means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document using said decrypted keys, wherein said selected ones of said encrypted elements are those which were encrypted for said key class; ~~and~~

~~said computer readable program code means for rendering further comprises:~~

~~computer readable program code means for rendering said decrypted selected ones and said other unencrypted elements~~.

Claim 22 (currently amended): The computer program product according to Claim 17, wherein:

said computer-readable program code means for decrypting said member-specific version further comprises:

~~said computer-readable program code means for contacting said group clerk further comprises:~~

computer-readable program code means for locating said ~~group~~ clerk process; and

computer-readable program code means for establishing a mutually-authenticated secure session between said client device and said ~~group~~ clerk process;

Q19

~~said computer-readable program code means for decrypting said different version for each of said determined communities further comprises:~~

computer-readable program code means for sending said member-specific ~~different~~ version to said ~~group~~ clerk process on said secure session;

computer-readable program code means for receiving said sent member-specific ~~different~~ version by said ~~group~~ clerk process;

computer-readable program code means for verifying, by said ~~group~~ clerk process, that said individual ~~requesting~~ user or process is one of said ~~authorized~~ members of said ~~determined community~~ identified group associated with said member-specific ~~different~~ version;

computer-readable program code means for decrypting said member-specific ~~different~~ version using a private key of said clerk process ~~one member which is associated with said public key which was used for encryption~~;

computer-readable program code means for returning said decrypted member-specific ~~different~~ version from said ~~group~~ clerk process to said client device on said secure session; and

computer-readable program code means for receiving said decrypted member-specific ~~different~~ version at said client device; and

said computer-readable program code means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document is executed at said client device using said received decrypted member-specific ~~different~~ version.

Claim 23 (currently amended): The computer program product according to Claim 17, Claim 21, or Claim 22, ~~wherein said computer-readable program code means for rendering further comprises~~ further comprising computer-readable program code means for substituting a predetermined ~~rendering a substitute~~ text message for any ~~of said selected~~ encrypted elements in said ~~requested~~ output document which cannot be decrypted ~~by said computer-readable program code means for decrypting said requested output document~~ for said individual user or process.

Claim 24 (currently amended): The computer program product according to Claim 19, ~~wherein~~ further comprising:

~~said~~ computer-readable program code means for contacting said ~~group~~ clerk process, further ~~comprises~~ comprising:

computer-readable program code means for programmatically locating said ~~group~~ clerk process; and

computer-readable program code means for establishing a session between said ~~client~~ a client device used by said individual user or process and said ~~group~~ clerk process; and wherein:

said computer-readable program code means for encrypting a separate version uses a public key of said clerk process as input when creating said member-specific version for said clerk process; and

said computer-readable program code means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document further comprises:

computer-readable program code means for locating said member-specific ~~different~~ version of said ~~random encryption~~ symmetric key which was encrypted using said public key of said ~~one member~~ clerk process, wherein said ~~one member~~ clerk process is associated with a ~~said expanded~~ group of which said individual ~~requesting~~ user or process is a group member; ~~one of said expanded group members;~~

computer-readable program code means for digitally signing, by said individual ~~requesting~~ user or process, said located version and an element encrypted with said member-specific ~~different~~ version, thereby creating a first digital signature;

computer-readable program code means for sending said first digital signature, said located member-specific ~~different~~ version, and said element to said ~~group~~ clerk process on said session;

computer-readable program code means for receiving said sent first digital signature, said member-specific ~~different~~ version, and said element by said ~~group~~ clerk process;

computer-readable program code means for verifying said first digital signature by said ~~group~~ clerk process;

computer-readable program code means for verifying, by said ~~group~~ clerk process, that said individual ~~requesting~~ user or process is one of said ~~authorized~~ members of said ~~determined community~~ identified group associated with said member-specific ~~different~~ version;

computer-readable program code means for decrypting said member-specific ~~different~~ version using a private key of said clerk process; ~~one member which is associated with said public key which was used for encryption;~~

computer-readable program code means for decrypting said element using said decrypted member-specific ~~different~~ version;

computer-readable program code means for re-encrypting said decrypted element using a public key of said individual ~~requesting~~ user or process, thereby creating a re-encrypted element;

computer-readable program code means for digitally signing said re-encrypted element by said ~~group~~ clerk process, thereby creating a second digital signature;

computer-readable program code means for returning said second digital signature and said re-encrypted element from said ~~group~~ clerk process to said client device on said session;

computer-readable program code means for receiving said second digital signature and said re-encrypted element at said client device; and

computer-readable program code means for verifying said second digital signature by said individual ~~requesting~~ user or process.

Claim 25 (original): The computer program product according to Claim 1, wherein said DTD is replaced by a schema.

Claim 26 (currently amended): The computer program product according to ~~Claim 10, wherein~~ Claim 1, wherein said encryption requirement further comprises specification of an encryption key length.

Claim 27 (original): The computer program product according to Claim 9, wherein said inserted encryption tags may surround either values of said elements or values and tags of said elements.

Claim 28 (currently amended): A system for enforcing security policy using style sheet processing in a computing environment, comprising:

means for obtaining an input document;

~~one or more stored policy enforcement objects, wherein each of said stored policy enforcement objects specifies a security policy to be associated with zero or more elements of said input document;~~

means for obtaining a Document Type Definition (DTD) ~~corresponding to~~ that defines elements of said input document, wherein: (1) an attribute of at least one element defined in said DTD ~~has been augmented with one or more~~ references ~~to selected ones~~ one of a plurality of ~~said~~

stored policy enforcement objects; (2) more than one of said references may reference a single stored policy enforcement object; and (3) each of said stored policy enforcement objects specifies a visibility policy for said referencing element or elements, said visibility policy identifying an encryption requirement for all elements having that visibility policy and a community whose members are authorized to view those elements;

means for applying one or more style sheets to said input document, thereby adding markup notation to each element of said input document for which said element definition in said DTD references one of said stored policy enforcement objects specifying a visibility policy with a non-null encryption requirement, resulting in creation of an interim transient document that indicates elements of said input document which are to be encrypted; and

Q19

means for creating an output document in which each element of said interim transient document for which markup notation has been added is encrypted in a manner that enables a clerk process associated with a group that is a community member authorized to view that element to use key distribution material associated with the output document when decrypting the encrypted element.

~~an augmented style sheet processor, wherein said augmented processor further comprises:~~

~~means for loading said DTD;~~

~~means for resolving each of said one or more references in said loaded DTD;~~

~~means for instantiating said policy enforcement objects associated with said resolved references;~~

~~means for executing selected ones of said instantiated policy enforcement objects during application of one or more style sheets to said input document, wherein a result of said means for executing is an interim transient document reflecting said execution;~~

~~means for generating one or more random encryption keys;~~

~~means for encrypting selected elements of said interim transient document, wherein a particular one of said generated random encryption keys may be used to encrypt one or more of said selected elements, while leaving zero or more other elements of said interim transient document unencrypted;~~

~~means for encrypting each of said one or more random encryption keys; and~~

~~means for creating an encrypted output document comprising said zero or more other unencrypted elements, said selected encrypted elements, and said encrypted encryption keys;~~

~~means for requesting, from a user or process on a client device, said encrypted output document, wherein said user or process is a member of a particular group authorized to view at least one of said selected encrypted elements;~~

~~means for receiving said requested output document at said client device; and~~

~~an augmented document processor executed on said client device, comprising:~~

~~means for contacting a clerk of said particular group for decryption of selected ones of said encrypted encryption keys; and~~

~~means for decrypting said requested output document using said decrypted selected ones of said encrypted encryption keys, thereby creating a result document.~~

Claim 29 (currently amended): The system according to Claim 28, further comprising means for rendering said output ~~result~~ document on ~~said client~~ a client device.

Claim 30 (currently amended): The system according to Claim 28, wherein said markup notation in said interim transient document comprises ~~one or more encryption~~ tags ~~identifying elements needing encryption~~ of a markup language.

Claim 31 (original): The system according to Claim 28, wherein said input document is specified in an Extensible Markup Language (XML) notation.

Claim 32 (currently amended): The system according to Claim 31, wherein said output ~~result~~ document is specified in said XML notation.

Claim 33 (currently amended): The system according to Claim 28, wherein said stored policy enforcement objects further comprise means for overriding a method for evaluating said elements of said input document, and wherein said means for applying said one or more style sheets ~~executing~~ further comprises means for invoking ~~executing~~ said means for overriding, thereby causing said markup notation to be added.

Claim 34 (original): The system according to Claim 33, wherein said style sheets are specified in an Extensible Stylesheet Language (XSL) notation.

Claim 35 (original): The system according to Claim 34, wherein said method is a value-of method of said XSL notation, and wherein said means for overriding said value-of method is by subclassing said value-of method.

Claim 36 (currently amended): The system according to Claim 33 ~~or Claim 35~~, wherein:

said ~~overridden~~ overriding method comprises:

means for generating said markup notation as encryption tags; and

means for inserting said generated encryption tags into said interim transient document to surround elements of said interim transient document for which said visibility policy of said elements in said input document have said non-null ~~are determined to require~~ encryption requirement; and

said means for creating said output document further comprises means for encrypting ~~selected elements encrypts~~ those elements surrounded by said inserted encryption tags.

Claim 37 (canceled)

Claim 38 (currently amended): The system according to ~~Claim 37, wherein~~ Claim 28, wherein said encryption requirement further comprises specification of an encryption algorithm to be used when encrypting elements having that visibility policy.

Claim 39 (currently amended): The system according to ~~Claim 37, wherein~~ Claim 28, wherein said encryption requirement further comprises specification of an encryption algorithm strength value to be used when encrypting elements having that visibility policy.

Claim 40 (currently amended): The system according to ~~Claim 37, wherein~~ Claim 28, wherein said means for creating said output document further comprises:

means for generating a distinct symmetric key for each unique one of said communities identified by said visibility policy in said stored policy objects for each of said elements of said input document; and

~~said~~ means for encrypting each of said distinct symmetric keys to create member-specific versions thereof, further comprising:

means for determining whether each of said members of said community for which said distinct symmetric key was generated is an individual or a group; and

means for encrypting a separate version of said distinct symmetric key for each determined individual and for a clerk process associated with each determined group. ~~encryption keys further comprises means for encrypting a different version of each of said random encryption keys for each of said one or more members of each of zero or more of said communities which uses said encryption key, and wherein each of said different versions is encrypted using a public key of said community member for which said different version was encrypted.~~

Claim 41 (currently amended): The system according to ~~Claim 37, wherein said encryption requirement may have a null value to indicate that said specified security policy does not require~~

~~encryption.~~ Claim 40, wherein said means for encrypting a separate version of said distinct symmetric key creates one of said member-specific versions using, as input, a public key of one of said determined individuals or a public key of said clerk process.

Claim 42 (currently amended): The system according to Claim 28, wherein said ~~means for encrypting selected~~ encrypted elements in said created output document are encrypted using ~~uses~~ a cipher block chaining mode encryption process.

Claim 43 (currently amended): The system according to Claim 40, further comprising:

a19

means for creating a key class for each of said unique ~~community~~ communities, wherein said key class is associated with each of said encrypted elements of said output document for which members of this unique community ~~is an~~ are authorized ~~viewer~~ viewers, and wherein said key class comprises: (1) ~~a strongest~~ an encryption algorithm identifier and key length used when encrypting ~~requirement of~~ said associated encrypted elements; (2) an identifier of each of said members of said unique community; and (3) one of said ~~different~~ member-specific versions of said encrypted symmetric ~~encryption~~ key for each of said identified community members~~; and~~

~~wherein:~~

~~said means for generating said one or more random encryption keys generates a particular one of said random encryption keys for each of said key classes, and wherein each of said different versions in a particular key class is encrypted from said generated encryption key generated for said key class; and~~

~~said means for encrypting selected elements uses that one of said particular random encryption keys which was generated for said key class with which said selected element is associated.~~

Claim 44 (currently amended): The system according to Claim 40, further comprising ~~wherein~~:

~~said~~ means for decrypting, for an individual user or process that is a member of one or more of said determined groups, only those encrypted elements in said ~~requested~~ output document for which any of said one or more of said determined groups is one of said authorized community members, further ~~comprises~~ comprising:

means for expanding said ~~one or more~~ determined groups ~~of said communities~~ to determine said individual users or processes that are group members in each of said expanded groups;

means for identifying ~~determining~~ one or more of said expanded groups ~~communities~~ of which said individual ~~requesting~~ user or process is one of said ~~expanded~~ group members;

means for decrypting, by said clerk process for each of said ~~determined communities~~ identified groups, said ~~different~~ member-specific version of said ~~random encryption~~ symmetric key ~~which was encrypted using said public key of said one member, wherein said one member is said expanded group of which said requesting user or process is one of said expanded group members~~, thereby creating a decrypted key for each of said ~~determined communities~~ identified groups; and

means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document using said decrypted keys, wherein said selected ones of said encrypted elements are those which were encrypted for one of said ~~determined communities~~ identified groups; ~~and~~

~~said means for rendering further comprises:~~

~~means for rendering said decrypted selected ones and said other unencrypted elements~~.

Claim 45 (currently amended): The system according to Claim 44, wherein:

said means for encrypting a separate version uses a public key of said clerk process as input when creating said member-specific version for said clerk process;

said means for decrypting said member-specific version of said symmetric key further comprises:

said means for contacting said ~~group~~ clerk process, further ~~comprises~~ comprising:

means for programmatically locating said ~~group~~ clerk process; and

means for establishing a session between ~~said client~~ a client device used by said individual user or process and said ~~group~~ clerk process;

~~said means for decrypting said different version for each of said determined communities further comprises:~~

means for digitally signing said ~~different~~ member-specific version by said individual ~~requesting~~ user or process, thereby creating a first digital signature;

means for sending said first digital signature and said ~~different~~ member-specific version to said ~~group~~ clerk process on said session;

means for receiving said sent first digital signature and said ~~different~~ member-specific version by said ~~group~~ clerk process;

means for verifying said first digital signature by said ~~group~~ clerk process;

means for verifying, by said ~~group~~ clerk process, that said ~~requesting~~ individual user or process is one of said ~~authorized~~ members of said ~~determined community~~ identified group associated with said ~~different~~ member-specific version;

means for decrypting said ~~different~~ member-specific version using a private key of said ~~one member which~~ clerk process, wherein said private key is associated with said public key ~~which was used for encryption~~ of said clerk process;

means for re-encrypting said decrypted ~~different~~ member-specific version using a public key of said individual ~~requesting~~ user or process, thereby creating a re-encrypted key;

means for digitally signing said re-encrypted key by said ~~group~~ clerk process, thereby creating a second digital signature;

means for returning said second digital signature and said re-encrypted key from said ~~group~~ clerk process to said client device on said session;

means for receiving said second digital signature and said re-encrypted key at said client device;

means for verifying said second digital signature at said client device; and

means, operable on said client device, for decrypting said received re-encrypted key using a private key of said individual ~~requesting~~ user or process, creating said decrypted key; and

said means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document is executed at said client device using said decrypted key.

Claim 46 (currently amended): The system according to Claim 40, ~~wherein~~ further comprising:

~~said~~ means for decrypting, for an individual user or process that is a member of one of said determined groups, only those encrypted elements in said ~~requested~~ output document for which any of said one or more of said determined groups is one of said authorized community members, further ~~comprises~~ comprising:

means for expanding said ~~one or more~~ determined groups ~~of said communities~~ to determine said individual users or processes that are group members in each of said expanded groups;

means for identifying ~~determining~~ one or more of said expanded groups ~~communities~~ of which said individual ~~requesting~~ user or process is one of said ~~expanded~~ group members; and

means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document, wherein said selected ones of said encrypted elements are those which were encrypted for one of said identified groups ~~determined communities; and~~

~~said means for rendering further comprises:~~

~~means for rendering said returned decrypted elements and said other unencrypted elements.~~

Claim 47 (currently amended): The system according to Claim 46, further comprising ~~wherein~~:

~~said~~ means for contacting said ~~group~~ clerk process, further ~~comprises~~ comprising:

means for programmatically locating said ~~group~~ clerk process; and

means for establishing a mutually-authenticated secure session between ~~said client~~ a client device used by said individual user or process and said ~~group~~ clerk process; and wherein:

said means for encrypting a separate version uses a public key of said clerk process as input when creating said member-specific version for said clerk process; and

said means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document further comprises:

means for locating said member-specific ~~different~~ version of said ~~random encryption~~ symmetric key which was encrypted using said public key of said ~~one member~~ clerk process, wherein said clerk process ~~one member~~ is associated with a ~~said expanded~~ group of which said individual ~~requesting~~ user or process is a group member; ~~one of said expanded group members;~~

19

means for sending said located member-specific ~~different~~ version to said ~~group~~ clerk process, along with an element encrypted with said member-specific ~~different~~ version, on said secure session;

means for receiving said sent member-specific ~~different~~ version and said element by said ~~group~~ clerk process;

means for verifying, by said ~~group~~ clerk process, that said ~~requesting~~ individual user or process is one of said ~~authorized~~ members of said ~~determined community~~ identified group associated with said member-specific ~~different~~ version;

means for decrypting said member-specific ~~different~~ version using a private key of said clerk process; ~~one member which is associated with said public key which was used for encryption;~~

means for decrypting said element using said decrypted member-specific ~~different~~ version; and

means for returning said decrypted element from said ~~group~~ clerk process to said client device on said secure session.

Claim 48 (currently amended): The system according to Claim 43, wherein: said means for encrypting a separate version uses a public key of said clerk process as input when creating said member-specific version for said clerk process; and further comprising:

~~said~~ means for contacting said ~~group~~ clerk process, further ~~comprises~~ comprising:

means for programmatically locating said ~~group~~ clerk process; and

means for establishing a mutually-authenticated secure session between ~~said client~~ a client device used by said individual user or process and said ~~group~~ clerk process;

~~said~~ means for decrypting, for an individual user or process that is a member of one of said determined groups, only those encrypted elements in said ~~requested~~ output document for which any of said one or more of said determined groups is one of said authorized community members, further comprising: ~~further comprises:~~

means for expanding said ~~one or more~~ determined groups ~~of said communities~~ to determine said individual users or processes that are group members in each of said expanded groups;

means for identifying ~~determining~~ one or more of said key classes which identify said ~~requesting~~ individual user or process as one of said ~~expanded~~ group members;

means for decrypting, for each of said determined key classes, said member-specific ~~different~~ version of said symmetric ~~random encryption~~ key in said key class which was encrypted using said public key of said clerk process ~~one member~~, wherein said means for decrypting uses a private key of said clerk process ~~one member which is associated with said public key which was used for encryption~~, thereby creating a decrypted key; and

means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document using said decrypted keys, wherein said selected ones of said encrypted elements are those which were encrypted for said key class~~; and~~

~~said means for rendering further comprises:~~

~~means for rendering said decrypted selected ones and said other unencrypted elements~~.

a19

Claim 49 (currently amended): The system according to Claim 44, wherein:

said means for decrypting said member-specific version further comprises:

~~said means for contacting said group clerk further comprises:~~

means for locating said ~~group~~ clerk process; and

means for establishing a mutually-authenticated secure session between said client device and said ~~group~~ clerk process;

~~said means for decrypting said different version for each of said determined communities further comprises:~~

means for sending said member-specific ~~different~~ version to said ~~group~~ clerk process on said secure session;

means for receiving said sent member-specific ~~different~~ version by said ~~group~~ clerk process;

means for verifying, by said ~~group~~ clerk process, that said individual ~~requesting~~ user or process is one of said ~~authorized~~ members of said ~~determined community~~ identified group associated with said member-specific ~~different~~ version;

means for decrypting said member-specific ~~different~~ version using a private key of said clerk process ~~one member which is associated with said public key which was used for encryption~~;

means for returning said decrypted member-specific ~~different~~ version from said ~~group~~ clerk process to said client device on said secure session; and

means for receiving said decrypted member-specific ~~different~~ version at said client device; and

said means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document is executed at said client device using said received decrypted member-specific ~~different~~ version.

Claim 50 (currently amended): The system according to Claim 44, Claim 48, or Claim 49, ~~wherein said means for rendering further comprises~~ further comprising means for substituting a predetermined ~~rendering a substitute~~ text message for any ~~of said selected~~ encrypted elements in

said ~~requested~~ output document which cannot be decrypted ~~by said means for decrypting said requested output document~~ for said individual user or process.

Claim 51 (currently amended): The system according to Claim 46, ~~wherein~~ further comprising:

~~said~~ means for contacting said ~~group~~ clerk process, further ~~comprises~~ comprising:

means for programmatically locating said ~~group~~ clerk process; and

means for establishing a session between ~~said client~~ a client device used by said individual user or process and said ~~group~~ clerk process; and wherein:

said means for encrypting a separate version uses a public key of said clerk process as input when creating said member-specific version for said clerk process; and

said means for decrypting selected ones of said encrypted elements in said ~~requested~~ output document further comprises:

means for locating said member-specific ~~different~~ version of said ~~random encryption~~ symmetric key which was encrypted using said public key of said ~~one member~~ clerk process, wherein said ~~one member~~ clerk process is associated with a ~~said expanded~~ group of which said individual ~~requesting~~ user or process is a group member; ~~one of said expanded group members;~~

means for digitally signing, by said individual ~~requesting~~ user or process, said located version and an element encrypted with said member-specific ~~different~~ version, thereby creating a first digital signature;

means for sending said first digital signature, said located member-specific ~~different~~ version, and said element to said ~~group~~ clerk process on said session;

means for receiving said sent first digital signature, said member-specific ~~different~~ version, and said element by said ~~group~~ clerk process;

means for verifying said first digital signature by said ~~group~~ clerk process;

means for verifying, by said ~~group~~ clerk process, that said individual ~~requesting~~ user or process is one of said ~~authorized~~ members of said ~~determined community~~ identified group associated with said member-specific ~~different~~ version;

means for decrypting said member-specific ~~different~~ version using a private key of said clerk process; ~~one member which is associated with said public key which was used for encryption;~~

means for decrypting said element using said decrypted member-specific ~~different~~ version;

means for re-encrypting said decrypted element using a public key of said individual ~~requesting~~ user or process, thereby creating a re-encrypted element;

means for digitally signing said re-encrypted element by said ~~group~~ clerk process, thereby creating a second digital signature;

means for returning said second digital signature and said re-encrypted element from said ~~group~~ clerk process to said client device on said session;

means for receiving said second digital signature and said re-encrypted element at said client device; and

means for verifying said second digital signature by said individual ~~requesting~~ user or process.

Claim 52 (original): The system according to Claim 28, wherein said DTD is replaced by a schema.

Claim 53 (currently amended): The system according to ~~Claim 37, wherein~~ Claim 28, wherein said encryption requirement further comprises specification of an encryption key length.

Claim 54 (original): The system according to Claim 36, wherein said inserted encryption tags may surround either values of said elements or values and tags of said elements.

a 19

Claim 55 (currently amended): A method for enforcing security policy using style sheet processing, comprising the steps of:

providing an input document;

~~providing one or more stored policy enforcement objects, wherein each of said stored policy enforcement objects specifies a security policy to be associated with zero or more elements of said input document;~~

providing a Document Type Definition (DTD) ~~corresponding to~~ that defines elements of said input document, wherein: (1) an attribute of at least one element defined in said DTD ~~has been augmented with one or more~~ references ~~to selected ones~~ one of a plurality of ~~said~~ stored policy enforcement objects; (2) more than one of said references may reference a single stored

policy enforcement object; and (3) each of said stored policy enforcement objects specifies a visibility policy for said referencing element or elements, said visibility policy identifying an encryption requirement for all elements having that visibility policy and a community whose members are authorized to view those elements;

applying one or more style sheets to said input document, thereby adding markup notation to each element of said input document for which said element definition in said DTD references one of said stored policy enforcement objects specifying a visibility policy with a non-null encryption requirement, resulting in creation of an interim transient document that indicates elements of said input document which are to be encrypted; and

creating an output document in which each element of said interim transient document for which markup notation has been added is encrypted in a manner that enables a clerk process associated with a group that is a community member authorized to view that element to use key distribution material associated with the output document when decrypting the encrypted element.

~~executing an augmented style sheet processor, further comprising the steps of:~~

~~loading said DTD;~~

~~resolving each of said one or more references in said loaded DTD;~~

~~instantiating said policy enforcement objects associated with said resolved references;~~

~~executing selected ones of said instantiated policy enforcement objects during application of one or more style sheets to said input document, wherein a result of said step of executing selected ones is an interim transient document reflecting said execution;~~

~~generating one or more random encryption keys;~~

~~encrypting selected elements of said interim transient document, wherein a particular one of said generated random encryption keys may be used to encrypt one or more of said selected elements, while leaving zero or more other elements of said interim transient document unencrypted;~~

~~encrypting each of said one or more random encryption keys; and~~

~~creating an encrypted output document comprising said zero or more other unencrypted elements, said selected encrypted elements, and said encrypted encryption keys;~~

~~requesting, from a user or process on a client device, said encrypted output document, wherein said user or process is a member of a particular group authorized to view at least one of said selected encrypted elements;~~

~~receiving said requested output document at said client device; and~~

~~executing an augmented document processor executed on said client device, further comprising the steps of:~~

~~contacting a clerk of said particular group for decryption of selected ones of said encrypted encryption keys; and~~

~~decrypting said requested output document using said decrypted selected ones of said encrypted encryption keys, thereby creating a result document.~~

Claim 56 (currently amended): The method according to Claim 55, further comprising the step of rendering said output ~~result~~ document on ~~said client~~ a client device.

Claim 57 (currently amended): The method according to Claim 55, wherein said markup notation in said interim transient document comprises ~~one or more encryption~~ tags ~~identifying elements needing encryption~~ of a markup language.

Claim 58 (original): The method according to Claim 55, wherein said input document is specified in an Extensible Markup Language (XML) notation.

Claim 59 (currently amended): The method according to Claim 58, wherein said output ~~result~~ document is specified in said XML notation.

Claim 60 (currently amended): The method according to Claim 55, wherein said stored policy enforcement objects further comprise executable code for overriding a method for evaluating said elements of said input document, and wherein said applying said one or more style sheets ~~executing selected ones~~ step further comprises overriding said method for evaluating by invoking said executable code, thereby causing said markup notation to be added.

a19

Claim 61 (original): The method according to Claim 60, wherein said style sheets are specified in an Extensible Stylesheet Language (XSL) notation.

Claim 62 (original): The method according to Claim 61, wherein said method is a value-of method of said XSL notation, and wherein said step of overriding said value-of method is by subclassing said value-of method.

Claim 63 (currently amended): The method according to Claim 60 ~~or Claim 62~~, wherein:

said step of overriding further comprises the steps of:

generating said markup notation as encryption tags; and

inserting said generated encryption tags into said interim transient document to surround elements of said interim transient document for which said visibility policy of said elements in said input document have said non-null ~~are determined to require~~ encryption requirement; and

said step of creating said output document further comprises the step of encrypting ~~selected elements encrypts~~ those elements surrounded by said inserted encryption tags.

Claim 64 (canceled)

Claim 65 (currently amended): The method according to ~~Claim 64, wherein~~ Claim 55, wherein said encryption requirement further comprises specification of an encryption algorithm to be used when encrypting elements having that visibility policy.

Claim 66 (currently amended): The method according to ~~Claim 64, wherein~~ Claim 2558, wherein said encryption requirement further comprises specification of an encryption algorithm strength value to be used when encrypting elements having that visibility policy.

Claim 67 (currently amended): The method according to ~~Claim 64, wherein~~ Claim 55, wherein said step of creating said output document further comprises the steps of:

~~generating~~ a distinct symmetric key for each unique one of said communities identified by said visibility policy in said stored policy objects for each of said elements of said input document; and

~~said step of~~ encrypting each of said distinct symmetric keys to create member-specific versions thereof, further comprising the steps of:

determining whether each of said members of said community for which said distinct symmetric key was generated is an individual or a group; and

encrypting a separate version of said distinct symmetric key for each determined individual and for a clerk process associated with each determined group. ~~encryption keys further comprises the step of encrypting a different version of each of said random encryption keys for each of said one or more members of each of zero or more of said communities which uses said encryption key , and wherein each of said different versions is encrypted using a public key of said community member for which said different version was encrypted.~~

a 19

Claim 68 (currently amended): The method according to ~~Claim 64, wherein said encryption requirement may have a null value to indicate that said specified security policy does not require encryption.~~ Claim 67, wherein said step of encrypting a separate version of said distinct symmetric key creates one of said member-specific versions using, as input, a public key of one of said determined individuals or a public key of said clerk process.

Claim 69 (currently amended): The method according to Claim 55, wherein said ~~step of encrypting selected~~ encrypted elements in said created output document are encrypted using ~~uses~~ a cipher block chaining mode encryption process.

Claim 70 (currently amended): The method according to Claim 67, further comprising the step of:

creating a key class for each of said unique ~~community~~ communities, wherein said key class is associated with each of said encrypted elements of said output document for which members of this unique community ~~is an~~ are authorized ~~viewer~~ viewers, and wherein said key class comprises: (1) ~~a strongest~~ an encryption algorithm identifier and key length used when encrypting ~~requirement of~~ said associated encrypted elements; (2) an identifier of each of said members of said unique community; and (3) one of said ~~different~~ member-specific versions of said encrypted symmetric ~~encryption~~ key for each of said identified community members; ~~and~~

~~wherein:~~

~~said step of generating said one or more random encryption keys generates a particular one of said random encryption keys for each of said key classes, and wherein each of said different versions in a particular key class is encrypted from said generated encryption key generated for said key class; and~~

~~said step of encrypting selected elements uses that one of said particular random encryption keys which was generated for said key class with which said selected element is associated.~~

Claim 71 (currently amended): The method according to Claim 67, further comprising the step of ~~wherein:~~

~~said step of~~ decrypting, for an individual user or process that is a member of one or more of said determined groups, only those encrypted elements in said ~~requested~~ output document for which any of said one or more of said determined groups is one of said authorized community members, further ~~comprises~~ comprising the steps of:

expanding said ~~one or more~~ determined groups ~~of said communities~~ to determine said individual users or processes that are group members in each of said expanded groups;

identifying ~~determining~~ one or more of said expanded groups ~~communities~~ of which said individual ~~requesting~~ user or process is one of said ~~expanded~~ group members;

decrypting, by said clerk process for each of said ~~determined communities~~ identified groups, said ~~different~~ member-specific version of said ~~random encryption~~ symmetric key ~~which was encrypted using said public key of said one member, wherein said one member is said expanded group of which said requesting user or process is one of said expanded group members,~~ thereby creating a decrypted key for each of said ~~determined communities~~ identified groups; and

decrypting selected ones of said encrypted elements in said ~~requested~~ output document using said decrypted keys, wherein said selected ones of said encrypted elements are those which were encrypted for one of said ~~determined communities~~ identified groups; ~~and~~

~~said step of rendering further comprises the step of:~~

~~rendering said decrypted selected ones and said other unencrypted elements.~~

Claim 72 (currently amended): The method according to Claim 71, wherein:

said step of encrypting a separate version uses a public key of said clerk process as input when creating said member-specific version for said clerk process;

said step of decrypting said member-specific version of said symmetric key further comprises the steps of:

~~said step of~~ contacting said ~~group~~ clerk process, further ~~comprises~~ comprising the steps of:

programmatically locating said ~~group~~ clerk process; and

establishing a session between ~~said client~~ a client device used by said individual user or process and said ~~group~~ clerk process;

~~said step of decrypting said different version for each of said determined communities further comprises the steps of:~~

a 19

digitally signing said ~~different~~ member-specific version by said individual ~~requesting~~ user or process, thereby creating a first digital signature;

sending said first digital signature and said ~~different~~ member-specific version to said ~~group~~ clerk process on said session;

receiving said sent first digital signature and said ~~different~~ member-specific version by said ~~group~~ clerk process;

verifying said first digital signature by said ~~group~~ clerk process;

verifying, by said ~~group~~ clerk process, that said ~~requesting~~ individual user or process is one of said ~~authorized~~ members of said ~~determined community~~ identified group associated with said ~~different~~ member-specific version;

decrypting said ~~different~~ member-specific version using a private key of said ~~one member which~~ clerk process, wherein said private key is associated with said public key ~~which was used for encryption~~ of said clerk process;

re-encrypting said decrypted ~~different~~ member-specific version using a public key of said individual ~~requesting~~ user or process, thereby creating a re-encrypted key;

digitally signing said re-encrypted key by said ~~group~~ clerk process, thereby creating a second digital signature;

returning said second digital signature and said re-encrypted key from said ~~group~~ clerk process to said client device on said session;

receiving said second digital signature and said re-encrypted key at said client device;

verifying said second digital signature at said client device; and

decrypting, at said client device, said received re-encrypted key using a private key of said individual ~~requesting~~ user or process, creating said decrypted key; and

said step of decrypting selected ones of said encrypted elements in said ~~requested~~ output document is executed at said client device using said decrypted key.

Claim 73 (currently amended): The method according to Claim 67, ~~wherein~~ further comprising the step of:

~~said step of~~ decrypting, for an individual user or process that is a member of one of said determined groups, only those encrypted elements in said ~~requested~~ output document for which

any of said one or more of said determined groups is one of said authorized community members, further ~~comprises~~ comprising the steps of:

expanding said ~~one or more~~ determined groups ~~of said communities~~ to determine said individual users or processes that are group members in each of said expanded groups;

identifying ~~determining~~ one or more of said expanded groups ~~communities~~ of which said individual ~~requesting~~ user or process is one of said ~~expanded~~ group members; and

decrypting selected ones of said encrypted elements in said ~~requested~~ output document, wherein said selected ones of said encrypted elements are those which were encrypted for one of said identified groups ~~determined communities; and~~

~~said step of rendering further comprises the step of:~~

~~rendering said returned decrypted elements and said other unencrypted elements.~~

a 19

Claim 74 (currently amended): The method according to Claim 73, further comprising the ~~wherein:~~

~~said~~ step of contacting said ~~group~~ clerk process, further ~~comprises~~ comprising the steps of:

programmatically locating said ~~group~~ clerk process; and

establishing a mutually-authenticated secure session between ~~said client~~ a client device used by said individual user or process and said ~~group~~ clerk process; and wherein:

said step of encrypting a separate version uses a public key of said clerk process as input when creating said member-specific version for said clerk process; and

said step of decrypting selected ones of said encrypted elements in said ~~requested~~ output document further comprises the steps of:

locating said member-specific ~~different~~ version of said ~~random encryption~~ symmetric key which was encrypted using said public key of said ~~one member~~ clerk process, wherein said clerk process ~~one member~~ is associated with a ~~said expanded~~ group of which said individual ~~requesting~~ user or process is a group member; ~~one of said expanded group members;~~

sending said located member-specific ~~different~~ version to said ~~group~~ clerk process, along with an element encrypted with said member-specific ~~different~~ version, on said secure session;

receiving said sent member-specific ~~different~~ version and said element by said ~~group~~ clerk process;

verifying, by said ~~group~~ clerk process, that said ~~requesting~~ individual user or process is one of said ~~authorized~~ members of said ~~determined community~~ identified group associated with said member-specific ~~different~~ version;

a19

decrypting said member-specific ~~different~~ version using a private key of said clerk process; ~~one member which is associated with said public key which was used for encryption;~~

decrypting said element using said decrypted member-specific ~~different~~ version; and

returning said decrypted element from said ~~group~~ clerk process to said client device on said secure session.

Claim 75 (currently amended): The method according to Claim 70, wherein:

said step of encrypting a separate version uses a public key of said clerk process as input when creating said member-specific version for said clerk process; and further comprising the steps of:

~~said step of~~ contacting said ~~group~~ clerk process, further ~~comprises~~ comprising the steps of:

programmatically locating said ~~group~~ clerk process; and

establishing a mutually-authenticated secure session between ~~said client~~ a client device used by said individual user or process and said ~~group~~ clerk process;

~~said~~ step of decrypting, for an individual user or process that is a member of one of said determined groups, only those encrypted elements in said ~~requested~~ output document for which any of said one or more of said determined groups is one of said authorized community members, further comprising ~~further comprises~~ the steps of:

a19

expanding said ~~one or more~~ determined groups ~~of said communities~~ to determine said individual users or processes that are group members in each of said expanded groups;

identifying ~~determining~~ one or more of said key classes which identify said ~~requesting~~ individual user or process as one of said ~~expanded~~ group members;

decrypting, for each of said determined key classes, said member-specific ~~different~~ version of said symmetric ~~random encryption~~ key in said key class which was encrypted using said public key of said clerk process ~~one member~~, wherein said step of decrypting uses a private key of said clerk process ~~one member which is associated with said public key which was used for encryption~~, thereby creating a decrypted key; and

decrypting selected ones of said encrypted elements in said ~~requested~~ output document using said decrypted keys, wherein said selected ones of said encrypted elements are those which were encrypted for said key class; ~~and~~

~~said step of rendering further comprises the step of:~~

~~rendering said decrypted selected ones and said other unencrypted elements.~~

Claim 76 (currently amended): The method according to Claim 71, wherein:

said step of decrypting said member-specific version further comprises the steps of:

~~said step of contacting said group clerk further comprises the steps of:~~

locating said ~~group~~ clerk process; and

establishing a mutually-authenticated secure session between said client device and said ~~group~~ clerk process;

a 19

~~said step of decrypting said different version for each of said determined communities further comprises the steps of:~~

sending said member-specific ~~different~~ version to said ~~group~~ clerk process on said secure session;

receiving said sent member-specific ~~different~~ version by said ~~group~~ clerk process;

verifying, by said ~~group~~ clerk process, that said individual ~~requesting~~ user or process is one of said ~~authorized~~ members of said ~~determined community~~ identified group associated with said member-specific ~~different~~ version;

decrypting said member-specific ~~different~~ version using a private key of said clerk process ~~one member which is associated with said public key which was used for encryption~~;

returning said decrypted member-specific ~~different~~ version from said ~~group~~ clerk process to said client device on said secure session; and

receiving said decrypted member-specific ~~different~~ version at said client device; and

said step of decrypting selected ones of said encrypted elements in said ~~requested~~ output document is executed at said client device using said received decrypted member-specific ~~different~~ version.

Claim 77 (currently amended): The method according to Claim 71, Claim 75, or Claim 76, ~~wherein said step of rendering further comprises~~ further comprising the step of substituting a predetermined ~~rendering a substitute~~ text message for any ~~of said selected~~ encrypted elements in said ~~requested~~ output document which cannot be decrypted ~~by said step of decrypting said requested output document~~ for said individual user or process.

a19

Claim 78 (currently amended): The method according to Claim 73, ~~wherein~~ further comprising the steps of:

~~said step of~~ contacting said ~~group~~ clerk process, further ~~comprises~~ comprising the steps of:

programmatically locating said ~~group~~ clerk process; and

establishing a session between ~~said client~~ a client device used by said individual user or process and said ~~group~~ clerk process; and wherein:

said step of encrypting a separate version uses a public key of said clerk process as input when creating said member-specific version for said clerk process; and

said step of decrypting selected ones of said encrypted elements in said ~~requested~~ output document further comprises the steps of:

locating said member-specific ~~different~~ version of said ~~random encryption~~ symmetric key which was encrypted using said public key of said ~~one member~~ clerk process, wherein said ~~one member~~ clerk process is associated with a ~~said expanded~~ group of which said individual ~~requesting~~ user or process is a group member; ~~one of said expanded group members;~~

digitally signing, by said individual ~~requesting~~ user or process, said located version and an element encrypted with said member-specific ~~different~~ version, thereby creating a first digital signature;

sending said first digital signature, said located member-specific ~~different~~ version, and said element to said ~~group~~ clerk process on said session;

a 19

receiving said sent first digital signature, said member-specific ~~different~~ version, and said element by said ~~group~~ clerk process;

verifying said first digital signature by said ~~group~~ clerk process;

verifying, by said ~~group~~ clerk process, that said individual ~~requesting~~ user or process is one of said ~~authorized~~ members of said ~~determined community~~ identified group associated with said member-specific ~~different~~ version;

decrypting said member-specific ~~different~~ version using a private key of said clerk process; ~~one member which is associated with said public key which was used for encryption;~~

decrypting said element using said decrypted member-specific ~~different~~ version;

re-encrypting said decrypted element using a public key of said individual ~~requesting~~ user or process, thereby creating a re-encrypted element;

digitally signing said re-encrypted element by said ~~group~~ clerk process, thereby creating a second digital signature;

returning said second digital signature and said re-encrypted element from said ~~group~~ clerk process to said client device on said session;

receiving said second digital signature and said re-encrypted element at said client device; and

verifying said second digital signature by said individual ~~requesting~~ user or process.

a19 Claim 79 (original): The method according to Claim 55, wherein said DTD is replaced by a schema.

Claim 80 (currently amended): The method according to ~~Claim 64, wherein~~ Claim 55, wherein said encryption requirement further comprises specification of an encryption key length.

Claim 81 (original): The method according to Claim 63, wherein said inserted encryption tags may surround either values of said elements or values and tags of said elements.